Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____А.А. Галкин
«06» 07. 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины)

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2022

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Стандарты информационной безопасности» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО 3++ и учебного плана по направлению подготовки 10.03.01 «Информационная безопасность». В процессе подготовки обеспечивается формирование у студентов обобщенного представления об актуальной, действующей на текущий момент нормативной базой в области информационной безопасности и действующих стандартов по информационной безопасности.

Задачей дисциплины «Стандарты информационной безопасности» является изучение процедур аттестации объектов информатизации и информационных систем; лицензирования деятельности в области информационной безопасности; проведения категорирования объектов информатизации, специальных проверок и обследований; сертификации в сфере защиты информации; формирования системы защиты информации в соответствии с действующими стандартами в области информационной безопасности.

В курсе рассматривается нормативная база и правоприменение федеральных законов в области проведения сертификации, лицензирования и аттестации объектов информатизации при деятельности, связанной с секретными и конфиденциальными сведениями. В курсе рассматриваются современные действующие международные и отечественные стандарты в области обеспечения защиты информации в информационных системах. Курс предусматривает овладение навыками практической деятельности в области правоприменения существующего законодательства в области защиты информации ограниченного доступа.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Стандарты информационной безопасности» относится к вариативной части, формируемой участниками образовательных отношений Блока Б1 (код Б1.В.02). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, практических занятий и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
ПК-2 Способен осуществлять управление защитой информации в автоматизированных системах	ПК-2.1.1	Знать нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации	Тестовые вопросы
	ПК-2.1.2	Знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ПК-2.1.3	Знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	

	ПК-2.2.1	Умеет организовывать процесс применения отечественных и зарубежных стандартов в области защиты информации для проектирования, разработки и оценки защищенности компьютерных систем	
	ПК-2.2.2	Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	
	ПК-2.2.3	Умеет анализировать и использовать в практической деятельности нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	
	ПК-2.2.4	Умеет определять подлежащие защите информационные ресурсы автоматизированных систем	
	ПК-2.2.5	Умеет классифицировать и оценивать угрозы информационной безопасности; контролировать эффективность принятых мер по защите информации в автоматизированных системах	
	ПК-2.3.1	Владеть навыками анализа информационной инфраструктуры информационной системы и ее безопасности на предмет соответствия действующим стандартам нормативно-правовым документам	
	ПК-2.3.2	Владеть навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	
ПК-4 Способен разрабатывать организационно-распорядительных документы по защите информации в автоматизированных системах	ПК-4.1.1	Знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Тестовые вопросы
	ПК-4.1.2	Знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	
	ПК-4.1.3	Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	
	ПК-4.2.1	Уметь классифицировать и оценивать угрозы информационной безопасности; контролировать эффективность принятых мер по защите информации в автоматизированных системах	
	ПК-4.3.1	Владеть навыками определения правил и процедур управления системой защиты информации автоматизированной системы	
	ПК-4.3.2	Владеть навыками определения правил и процедур выявления инцидентов	
	ПК-4.3.3	Владеть навыками определения правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы	
	ПК-4.3.4	Владеть навыками определения правил и процедур реагирования на инциденты	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	**Раздел 1.** Стандарты информационной безопасности.	4	1	2	2				
2	**Раздел 2.** Стандарты информационной безопасности. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT.	4	2	2	2			3	
3	**Раздел 3.** Стандарты по безопасности информационных технологий в России.	4	3	2	2				
4	**Раздел 4.** Оценка безопасности информационных технологий на основе «Общих критериев».	4	4	2	2				
5	**Раздел 5.** Оценка уровня доверия функциональной безопасности информационной технологии.	4	5	2	2				
6	**Раздел 6.** Международный стандарт управления информационной безопасностью ISO 17799.	4	6	2	2				Рейтинг-контроль №1
7	**Раздел 7.** Международный стандарт управления информационной безопасностью ISO 17799. Части 3-5.	4	7	2	2				
8	**Раздел 8.** Международный стандарт управления информационной безопасностью ISO 17799. Части 6-7.	4	8	2	2				
9	**Раздел 9.** Международный стандарт управления ИБ ISO 17799. Части 8-10.	4	9	2	2				

10	**Раздел 10.** Программные средства для проведения аудита информационной безопасности. Система CRAMM.	4	10	2	2				
11	**Раздел 11.** Программные средства для проведения аудита информационной безопасности. Система КОНДОР.	4	11	2	2				
12	**Раздел 12.** Методика проведения аудита информационной безопасности на предприятии.	4	12	2	2				Рейтинг-контроль №2
13	**Раздел 13.** Организация и проведения работ по аудиту. Алгоритм проведения аудита безопасности предприятия.	4	13	2	2				
14	**Раздел 14.** Правовая основа системы стандартизации, лицензирования и сертификации в РФ.	4	14	2	2				
15	**Раздел 15.** Аттестация объектов информации.	4	15	2	2			3	
16	**Раздел 16.** Сертификация в области защиты информации.	4	16	2	2				
17	**Раздел 17.** Обзор основных нормативных документов государственных регуляторов в области информационной безопасности.	4	17	2	2			3	
18	**Раздел 18.** Ответственность за нарушения законодательства в сфере нарушений лицензирования и сертификации в РФ.	4	18	2	2				Рейтинг-контроль №3
Итого по дисциплине		**108**		**36**	**36**			**9**	**Экзамен 27**

Содержание лекционных занятий по дисциплине

Раздел 1. Стандарты информационной безопасности. Предпосылки создания стандартов ИБ. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран. Германский стандарт BS1.

Раздел 2. Стандарты информационной безопасности. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT.

Раздел 3. Стандарты по безопасности информационных технологий в России.

Раздел 4. Оценка безопасности информационных технологий на основе «Общих критериев». Предпосылки введения международного стандарта ISO 1540883. Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям.

Раздел 5. Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств общих критериев.

Раздел 6. Международный стандарт управления информационной безопасностью ISO 17799. Назначение стандарта ISO 17799 для управления информационной безопасностью. Практика прохождения аудита и получения сертификата ISO 17799. Часть 1. Политика безопасности. Часть 2. Организационные меры по обеспечению информационной безопасности.

Раздел 7. Международный стандарт управления информационной безопасностью ISO 17799. Часть 3. Классификация ресурсов и их контроль. Часть 4. Безопасность персонала. Часть 5. Физическая безопасность.
Раздел 8. Международный стандарт управления информационной безопасностью ISO 17799. Часть 6. Администрирование компьютерных систем и вычислительных сетей. Часть 7. Управление доступом к системам.
Раздел 9. Международный стандарт управления информационной безопасностью ISO 17799. Часть 8. Разработка и сопровождение информационных систем. Часть 9. Планирование бесперебойной работы организации. Часть 10. Соответствие системы основным требованиям.
Раздел 10. Программные средства для проведения аудита информационной безопасности. Анализ видов используемых программных продуктов. Система CRAMM.
Раздел 11. Программные средства для проведения аудита информационной безопасности. Система КОНДОР. Использование сетевых сканеров.
Раздел 12. Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ. Планирование процедуры аудита ИБ.
Раздел 13. Методика проведения аудита информационной безопасности на предприятии. Организация и проведения работ по аудиту. Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.
Раздел 14. Правовая основа системы стандартизации, лицензирования и сертификации в РФ. Лицензирующие органы в области защиты информации. Лицензирование в области защиты информации.
Раздел 15. Аттестация объектов информации. Проведение специальных проверок, специальных обследований и специальных исследований.
Раздел 16. Сертификация в области защиты информации.
Раздел 17. Обзор основных нормативных документов государственных регуляторов в области информационной безопасности.
Раздел 18. Ответственность за нарушения законодательства в сфере нарушений лицензирования и сертификации в РФ.

Содержание практических занятий по дисциплине

Практическая работа №1. Практика прохождения лицензирования деятельности в области обеспечения ИБ
Практическая работа №2. Практика прохождения сертификации деятельности в области обеспечения ИБ
Практическая работа №3. Меры ответственности за нарушения в области лицензирования и сертификации при обеспечении информационной безопасности
Практическая работа №4. Порядок аттестации объектов информатизации
Практическая работа №5. Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации
Практическая работа №6. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии
Практическая работа №7. Изучение требований и рекомендации по технической защите конфиденциальной информации (СТР-К) -2001. Изучение документа ФСТЭК РФ Р.2010.08.31.489. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования
Практическая работа №8. Изучение документа ФСТЭК РФ приказ №17-2013 и приказа №27-2017 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Изучение документа ФСТЭК РФ RD.1992.03.30.1. Руководящий документ

автоматизированные системы. Защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации.

Практическая работа №9. Изучение документа ФСТЭК РФ RD.1992.03.30.4. Руководящий документ концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Изучение требований методики оценки угроз безопасности информации ФСТЭК России (утверждена 05.02.2021).

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Перечень вопросов к рейтинг-контролю №1

- Стандарты информационной безопасности. Предпосылки создания стандартов ИБ. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран.
- Стандарты информационной безопасности. Германский стандарт BS1.
- Стандарты информационной безопасности. Британский стандарт BS 7799.
- Международный стандарт ISO 17799.
- Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT.
- Стандарты по безопасности информационных технологий в России.
- Оценка безопасности информационных технологий на основе «Общих критериев». Предпосылки введения международного стандарта ISO 1540883. Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям.
- Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств общих критериев.
- Международный стандарт управления информационной безопасностью ISO 17799. Назначение стандарта ISO 17799 для управления информационной безопасностью. Практика прохождения аудита и получения сертификата ISO 17799. Часть 1. Политика безопасности. Часть 2. Организационные меры по обеспечению информационной безопасности.
- Международный стандарт управления информационной безопасностью ISO 17799. Часть 3. Классификация ресурсов и их контроль. Часть 4. Безопасность персонала. Часть 5. Физическая безопасность.
- Международный стандарт управления информационной безопасностью ISO 17799. Часть 6. Администрирование компьютерных систем и вычислительных сетей. Часть 7. Управление доступом к системам.

Перечень вопросов к рейтинг-контролю №2

- Международный стандарт управления информационной безопасностью ISO 17799. Часть 3. Классификация ресурсов и их контроль. Часть 4. Безопасность персонала. Часть 5. Физическая безопасность.
- Международный стандарт управления информационной безопасностью ISO 17799. Часть 6. Администрирование компьютерных систем и вычислительных сетей. Часть 7. Управление доступом к системам.
- Международный стандарт управления информационной безопасностью ISO 17799. Часть 8. Разработка и сопровождение информационных систем. Часть 9. Планирование бесперебойной работы организации. Часть 10. Соответствие системы основным требованиям.

- Программные средства для проведения аудита информационной безопасности. Анализ видов используемых программных продуктов. Система CRAMM.
- Программные средства для проведения аудита информационной безопасности. Система КОНДОР.
- Программные средства для проведения аудита информационной безопасности. Использование сетевых сканеров.
- Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ.
- Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ. Планирование процедуры аудита ИБ.
- Методика проведения аудита информационной безопасности на предприятии. Организация и проведения работ по аудиту.
- Алгоритм проведения аудита информационной безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.
- Правовая основа системы стандартизации, лицензирования и сертификации в РФ.

Перечень вопросов к рейтинг-контролю №3

- Методика проведения аудита информационной безопасности на предприятии. Организация и проведения работ по аудиту.
- Алгоритм проведения аудита информационной безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.
- Правовая основа системы стандартизации, лицензирования и сертификации в РФ.
- Лицензирующие органы в области защиты информации. Лицензирование в области защиты информации.
- Организационная структура системы сертификации в области защиты конфиденциальной информации.
- При каких организациях созданы системы сертификации в РФ?
- Порядок и требования при осуществлении сертификации средств защиты информации.
- В каких случаях сертификация носит добровольный характер?
- Кем устанавливаются формы сертификата и знака соответствия?
- Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСТЭК?
- Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСБ?
- Аттестация объектов информации. Проведение специальных проверок, специальных обследований и специальных исследований.
- Сертификация в области защиты информации.
- Обзор основных нормативных документов государственных регуляторов в области информационной безопасности.
- Ответственность за нарушения законодательства в сфере нарушений лицензирования и сертификации в РФ.

5.2. Промежуточная аттестация

Примерный перечень вопросов к зачету

1. Стандарты информационной безопасности. Предпосылки создания стандартов ИБ. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран.

2. Стандарты информационной безопасности. Германский стандарт BS1.
3. Стандарты информационной безопасности. Британский стандарт BS 7799.
4. Международный стандарт ISO 17799.
5. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT.
6. Стандарты по безопасности информационных технологий в России.
7. Оценка безопасности информационных технологий на основе «Общих критериев». Предпосылки введения международного стандарта ISO 1540883.
8. Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям.
9. Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств общих критериев.
10. Международный стандарт управления информационной безопасностью ISO 17799. Назначение стандарта ISO 17799 для управления информационной безопасностью. Практика прохождения аудита и получения сертификата ISO 17799. Часть 1. Политика безопасности. Часть 2. Организационные меры по обеспечению информационной безопасности.
11. Международный стандарт управления информационной безопасностью ISO 17799. Часть 3. Классификация ресурсов и их контроль. Часть 4. Безопасность персонала. Часть 5. Физическая безопасность.
12. Международный стандарт управления информационной безопасностью ISO 17799. Часть 6. Администрирование компьютерных систем и вычислительных сетей. Часть 7. Управление доступом к системам.
13. Международный стандарт управления информационной безопасностью ISO 17799. Часть 8. Разработка и сопровождение информационных систем. Часть 9. Планирование бесперебойной работы организации. Часть 10. Соответствие системы основным требованиям.
14. Программные средства для проведения аудита информационной безопасности. Анализ видов используемых программных продуктов. Система CRAMM.
15. Программные средства для проведения аудита информационной безопасности. Система КОНДОР.
16. Программные средства для проведения аудита информационной безопасности. Использование сетевых сканеров.
17. Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ.
18. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ. Планирование процедуры аудита ИБ.
19. Методика проведения аудита информационной безопасности на предприятии. Организация и проведения работ по аудиту.
20. Алгоритм проведения аудита информационной безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.
21. Правовая основа системы стандартизации, лицензирования и сертификации в РФ.
22. Лицензирующие органы в области защиты информации. Лицензирование в области защиты информации.
23. Организационная структура системы сертификации в области защиты конфиденциальной информации.
24. При каких организациях созданы системы сертификации в РФ?
25. Порядок и требования при осуществлении сертификации средств защиты информации.
26. В каких случаях сертификация носит добровольный характер?
27. Кем устанавливаются формы сертификата и знака соответствия?
28. Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСТЭК?

29. Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСБ?
30. Аттестация объектов информации. Проведение специальных проверок, специальных обследований и специальных исследований.
31. Сертификация в области защиты информации.
32. Обзор основных нормативных документов государственных регуляторов в области информационной безопасности.
33. Ответственность за нарушения законодательства в сфере нарушений лицензирования и сертификации в РФ.

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов

1. Изучение «Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (утверждена постановлением правительства РФ от 06.02.2010 №63);
2. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии;
3. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации при ее обработке на средствах вычислительной техники;
4. Изучение порядка аттестации объектов информатизации;
5. Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации;
6. Изучение порядка проведения организационных и технических мероприятий по ТЗИ на ОИ;
7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) -2001;
8. Изучение документа ФСТЭК РФ Р_1994.11.25. Положение по аттестации объектов информатизации по требованиям безопасности информации;
9. Изучение документа ФСТЭК РФ Р_2010.08.31_489. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования;
10. Изучение документа ФСТЭК РФ приказ №17 от 11.02.2013 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
11. Изучение документа ФСТЭК РФ RD_1992.03.30_1. Руководящий документ автоматизированные системы. Защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации;
12. Изучение документа ФСТЭК РФ RD_1992.03.30_3. Руководящий документ защита от несанкционированного доступа к информации. термины и определения;
13. Изучение документа ФСТЭК РФ RD_1992.03.30_4. Руководящий документ концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Стандартизация. Международные стандарты

BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management
BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности

ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
ISO/IEC 27000 — Словарь и определения.
ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

Государственные (национальные) стандарты РФ

ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

Руководящие документы

РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации - содержит описание показателей защищенности информационных систем и требования к классам защищенности.
Стандарт Банка России СТО БР ИББС-1.0-2014 - Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
PCI DSS (Payment Card Industry Data Security Standard) - Стандарт безопасности данных индустрии платёжных карт.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 269 с. ISBN 978-5-9765-1256-6.	2016	https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 25.08.2021)
Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие: [16+] / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. – Москва: Прометей, 2018. – 173 с.	2018	https://biblioclub.ru/index.php?page=book&id=494850 (дата обращения: 27.08.2021)
Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с. ISBN 978-5-4499-0496-6. – DOI 10.23681/571485	2020	https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 27.08.2021)
Шилов, А. К. Управление информационной безопасностью: учебное пособие: [16+] / А. К. Шилов; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. ISBN 978-5-9275-2742-7	2018	https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 27.08.2021)
Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий: учебное пособие: [16+] / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – 140 с. ISBN 978-5-9275-3546-0	2020	https://biblioclub.ru/index.php?page=book&id=612162 (дата обращения: 27.08.2021)
Дополнительная литература		
Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие: [16+] / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с.	2017	https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 27.08.2021)
Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 269 с. ISBN 978-5-9765-1256-6	2016	https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 27.08.2021)
Брюхомицкий, Ю. А. Безопасность информационных технологий: учебное пособие: в 2 частях: [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – Ч. 1. – 171 с. ISBN 978-5-9275-3571-2 (Ч. 1). - ISBN 978-5-9275-3526-2. –	2020	https://biblioclub.ru/index.php?page=book&id=612167 (дата обращения: 27.08.2021)
Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов: [16+] / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – 4-е изд., стер. – Москва: ФЛИНТА, 2016. – 224 с. ISBN 978-5-9765-1274-0	2016	https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 27.08.2021)

6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html
2. Электронный журнал «Спецтехника и Связь», Режим доступа: http://www.st-s.su/

3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: http://sccs.intelgr.com/
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: http://www.ess.ru/
5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: http://asbgroup.ru/izdaniya/zhurnal-bdi/

6.3. Интернет-ресурсы

1. ООО "Издательский Дом «Интеллектуальная пресса» журнал «Интеллектуальная собственность. Авторское право и смежные права». Режим доступа: http://superpressa.ru/index.php?option=com_content&view=article&id=357&Itemid=111;
2. Журнал «Право интеллектуальной собственности» Издательская группа «Юрист», г. Москва. Режим доступа: http://pravois.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил _____ доцент кафедры ИЗИ Тельный А.В.
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр» _____ к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 14 от 28.06.22 года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»

Протокол № 14 от 28.06.22 года
Председатель комиссии д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, должность, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Стандарты информационной безопасности

образовательной программы направления подготовки *10.03.01 «Информационная безопасность»*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/ _____

Подпись *ФИО*